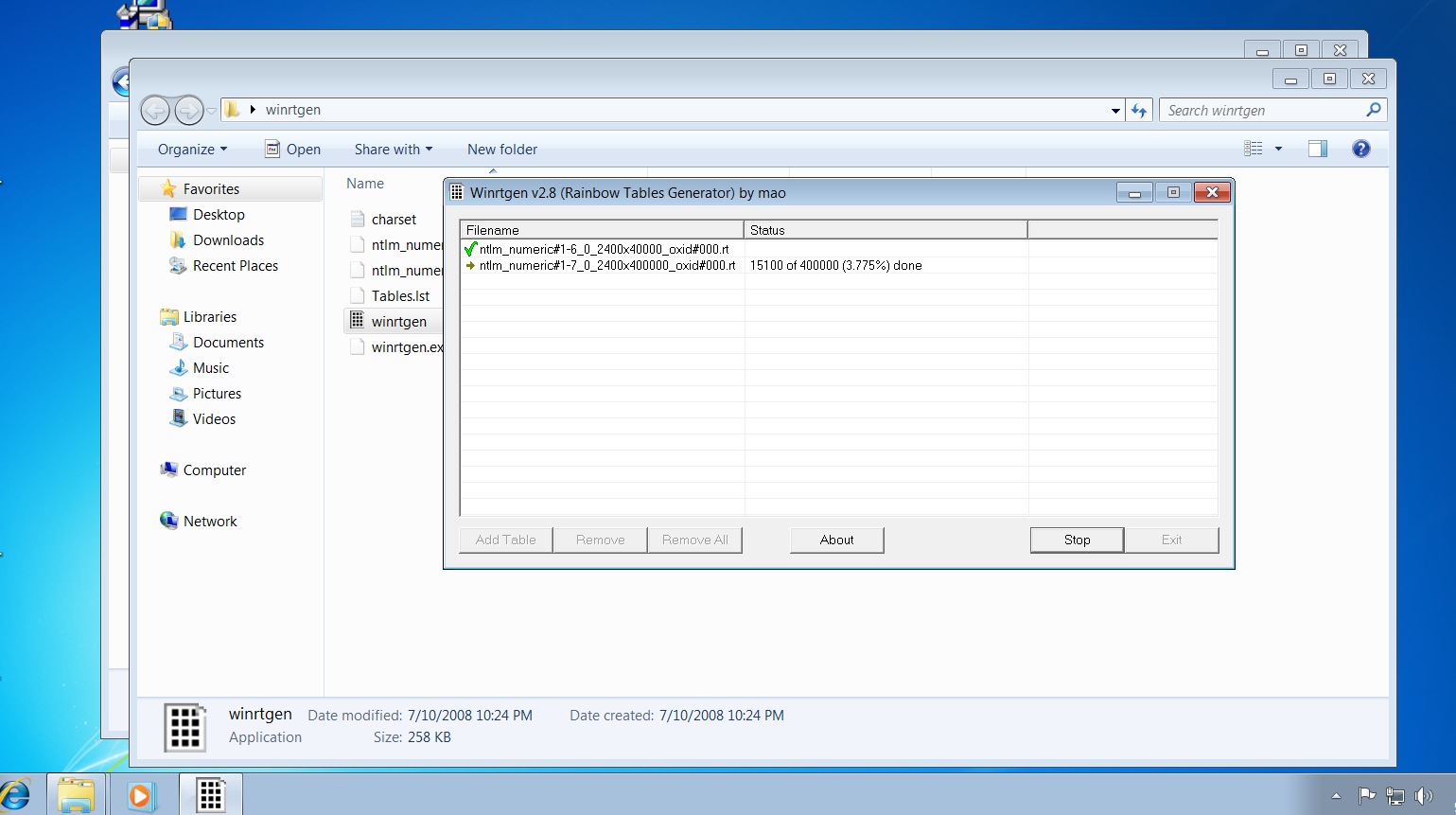
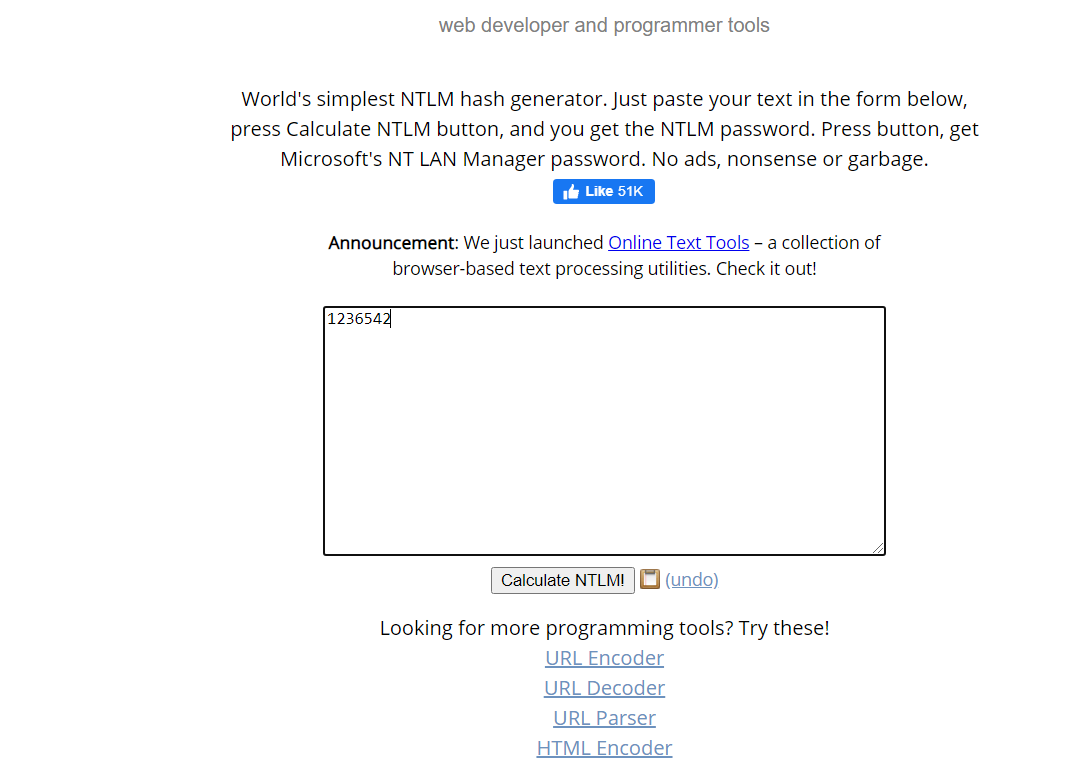
1. Rainbow Table

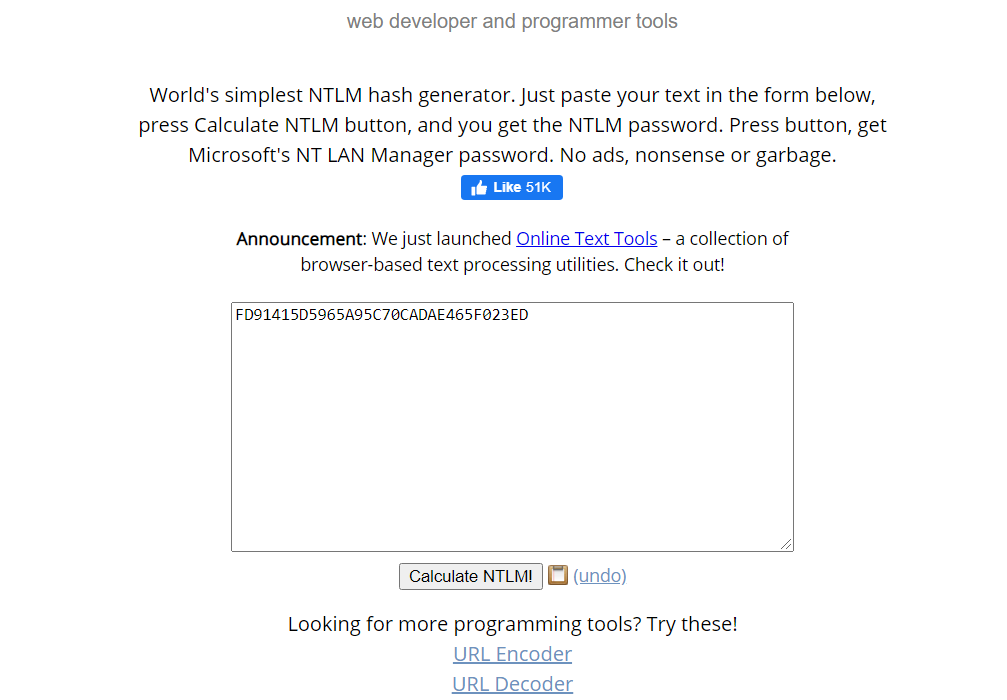
Chạy tool Winrtgen tạo Rainbow Table cho tool Rainbowcrack

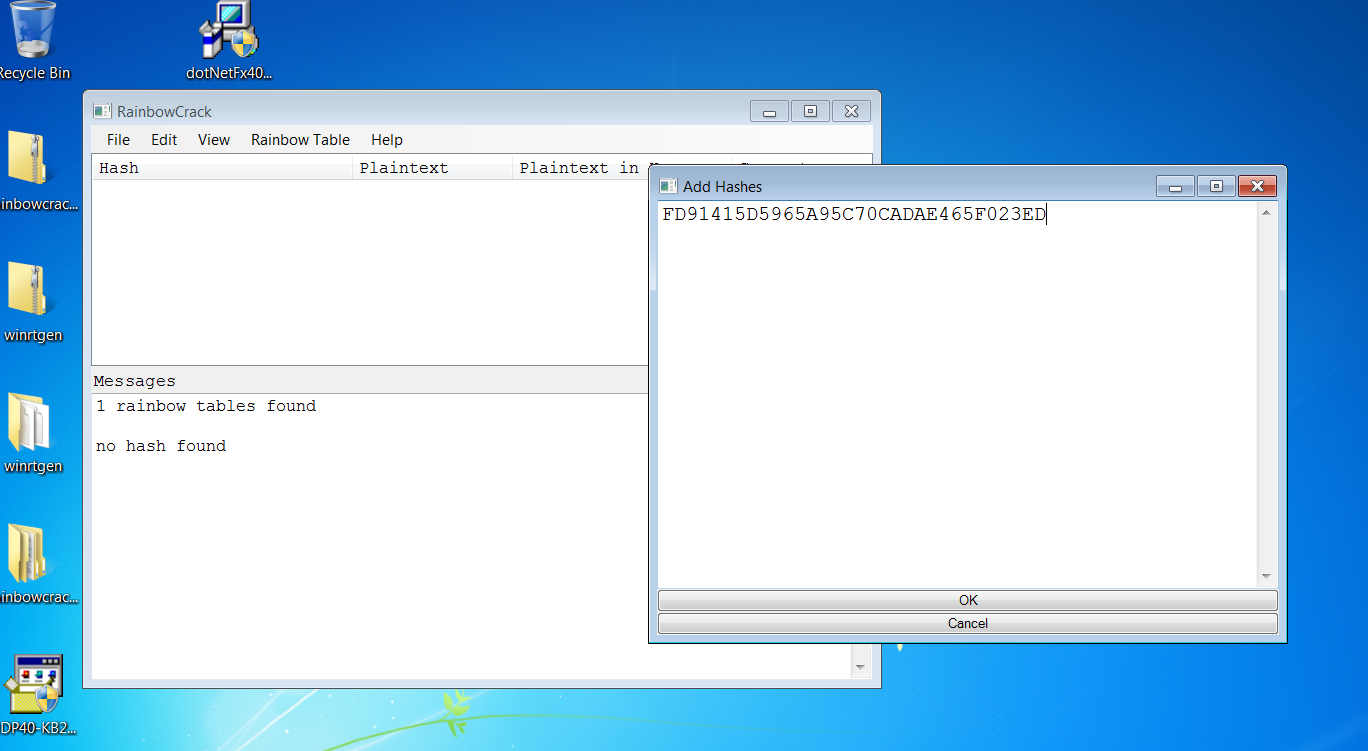
Chọn loại mã hoá hash ntlm độ dài passwork 7

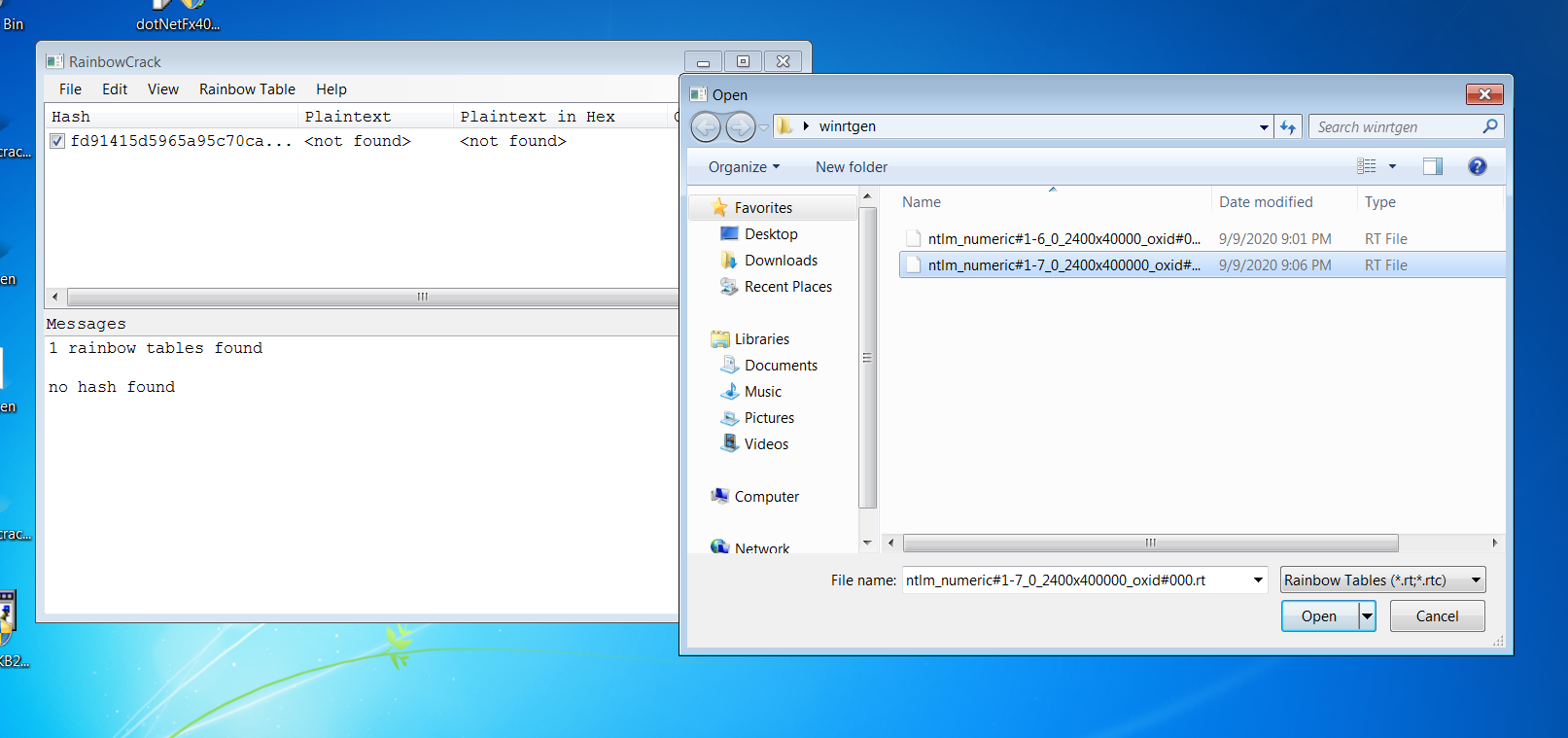


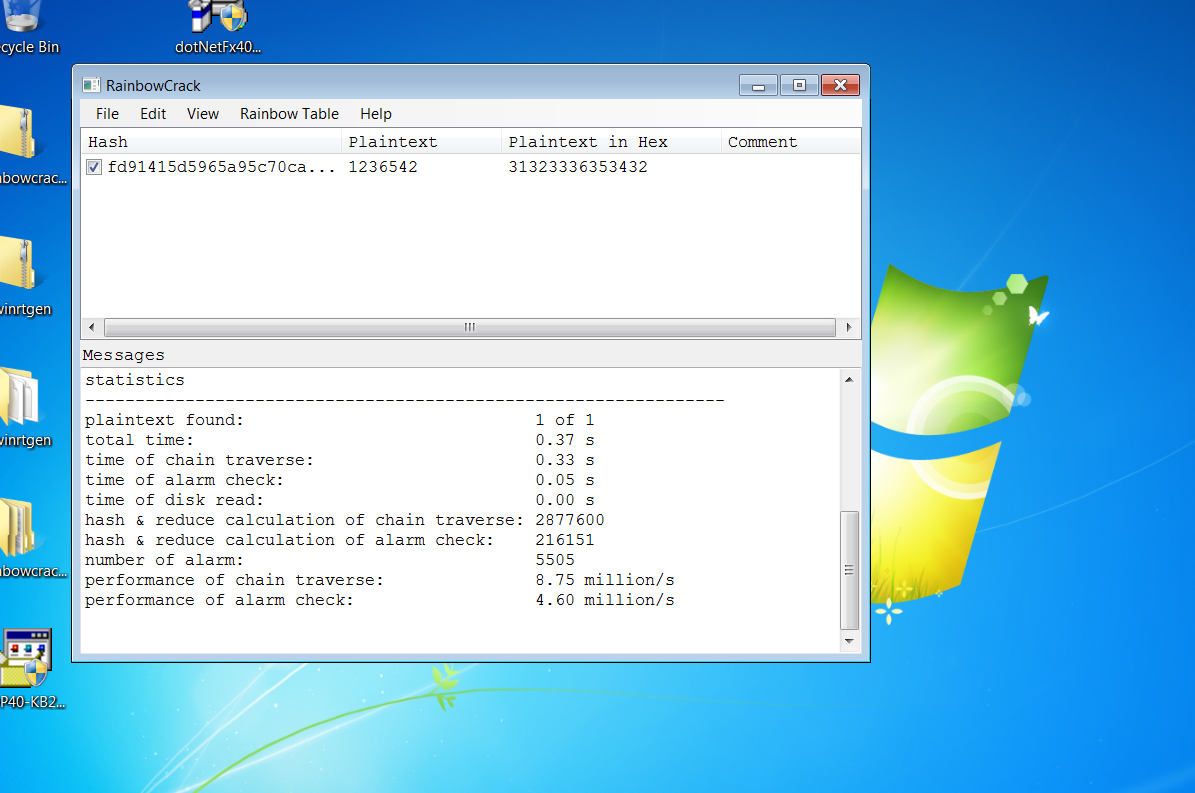






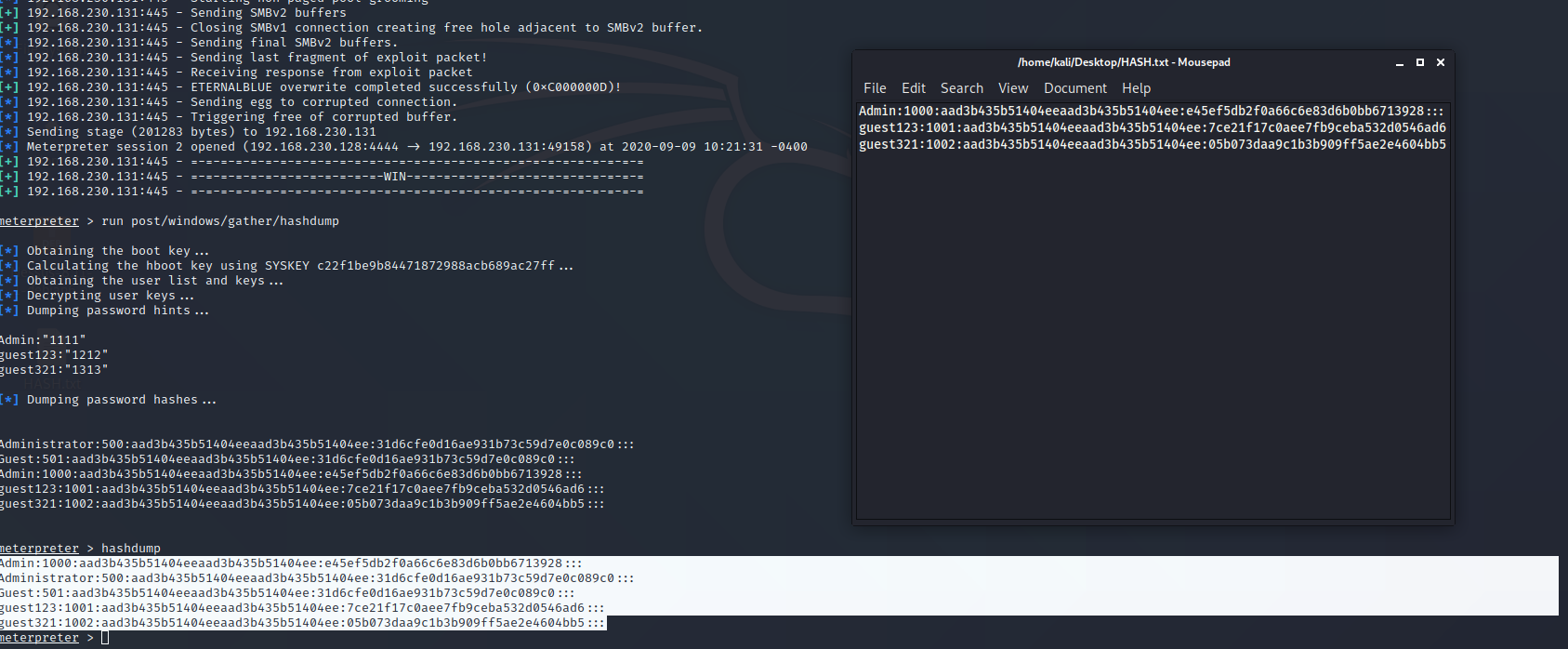




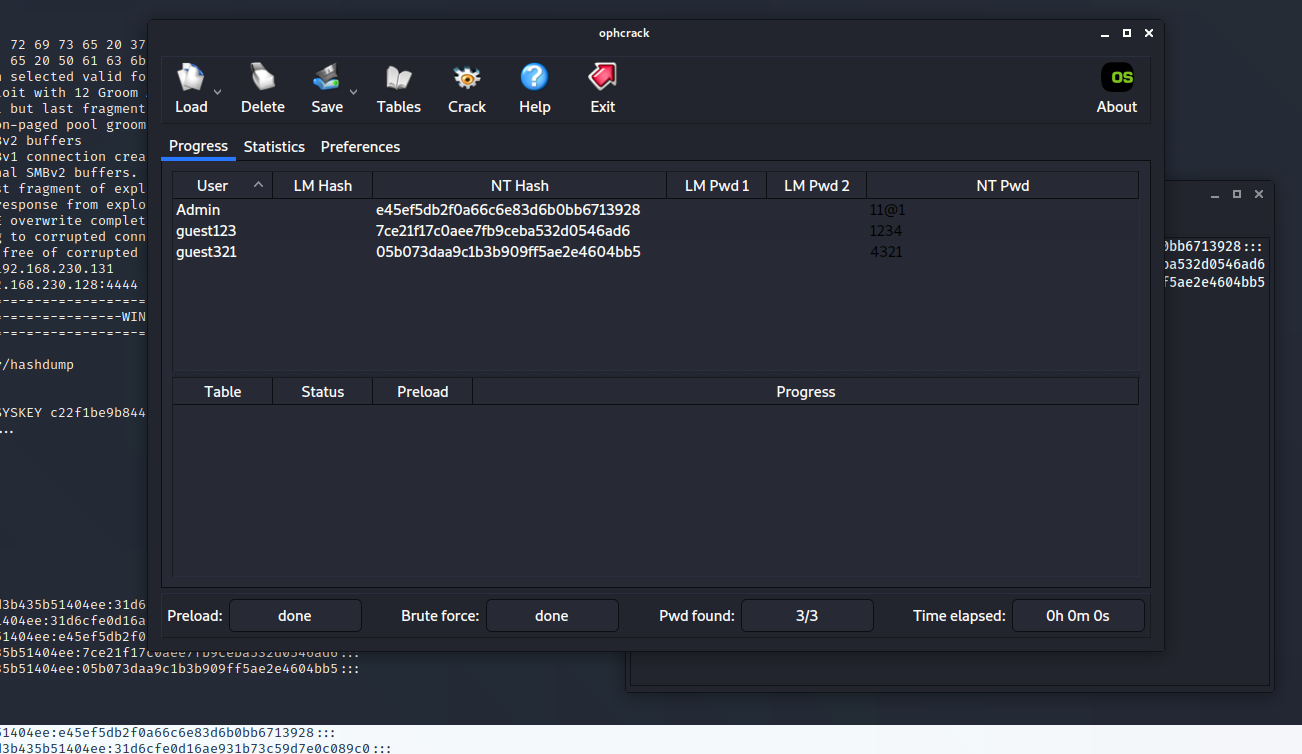


1. Password cracking

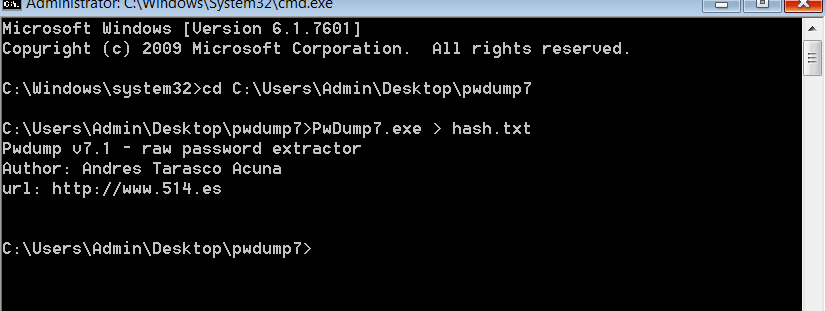
Với lỗ hổng ms17-010 trên win7; sử dụng máy ảo kali kết nối LAN với máy ảo win 7 dùng Metasploit tấn công lỗ hổng lấy thông tin file SAM trong máy ảo win 7 copy lưu vào file .txt



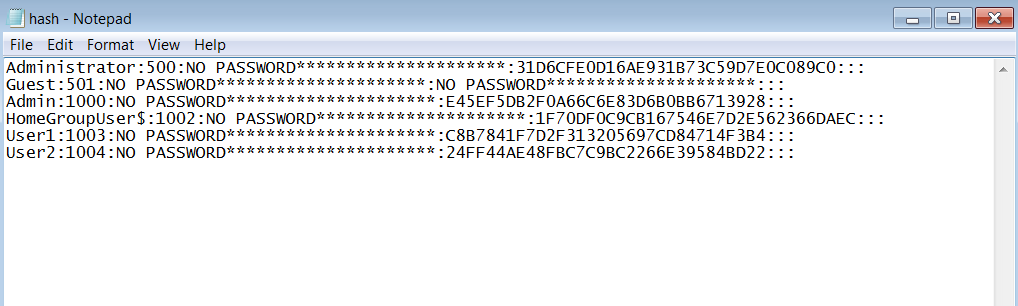
Mở tool Ophcrack dump file SAM ra password của các users



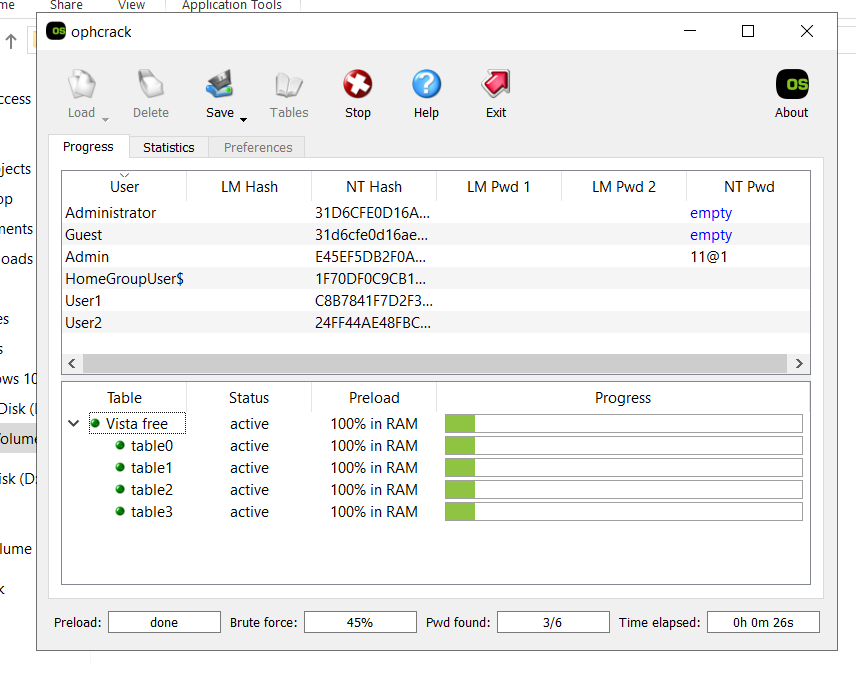
Dùng pwdump7 lấy dump file Sam



Lưu vào file hash.txt

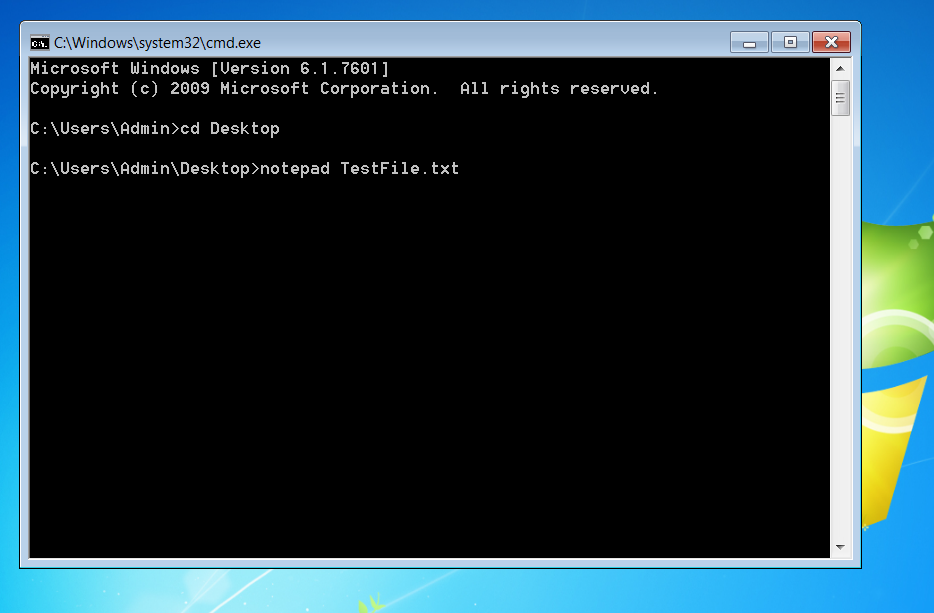


Chạy ophcrack trên win 10 để lấy password từ file hash vừa lấy

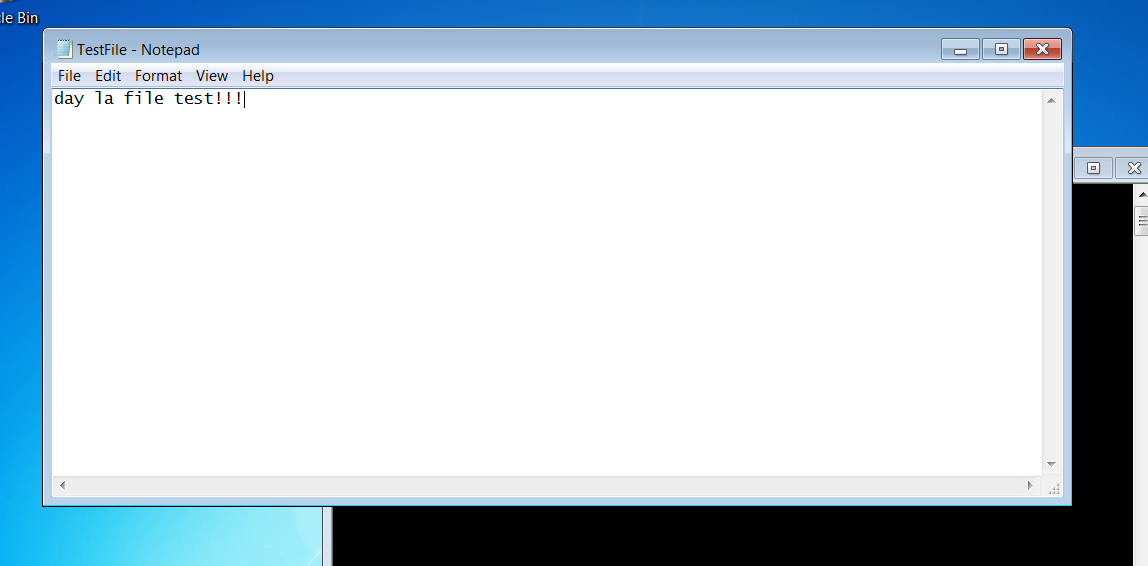


1. NTFS Steam

Ở dòng lệnh, nhập " **notepad Testfile.txt** ". Nó sẽ mở ra một notepad với một tệp văn bản mang tên TestFile.

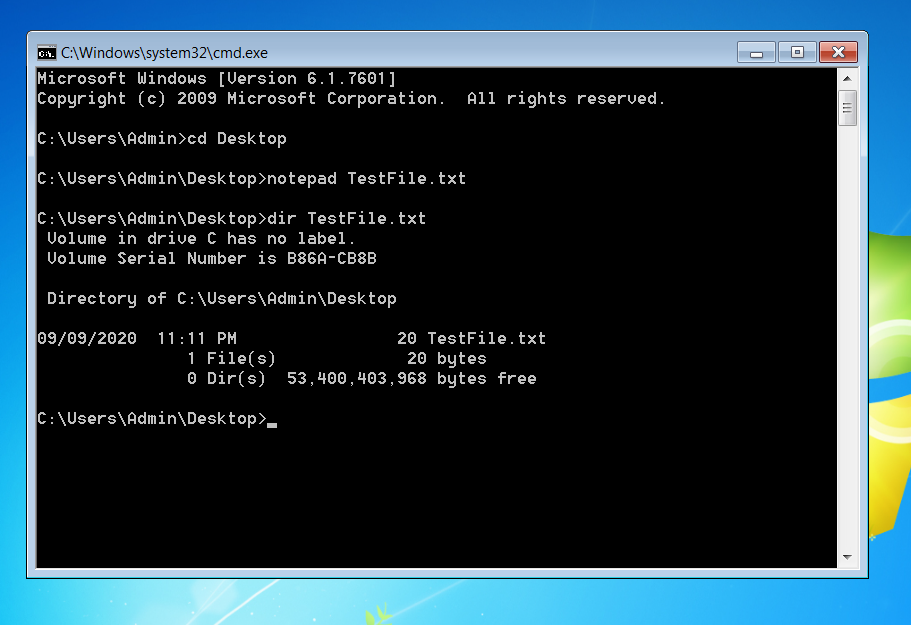


Nhập dữ liệu vào tệp.

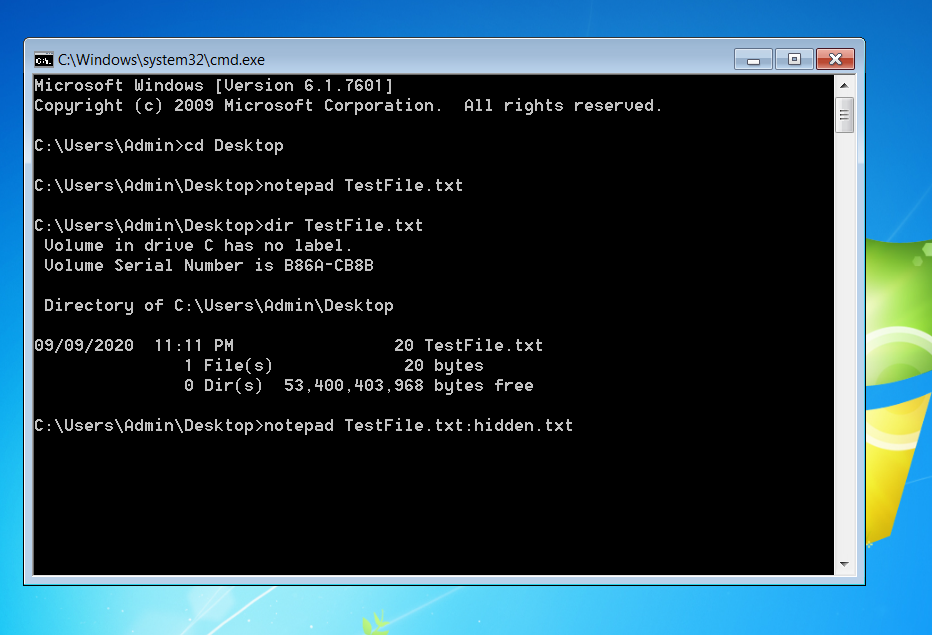


Lưu tệp và đóng Notepad.

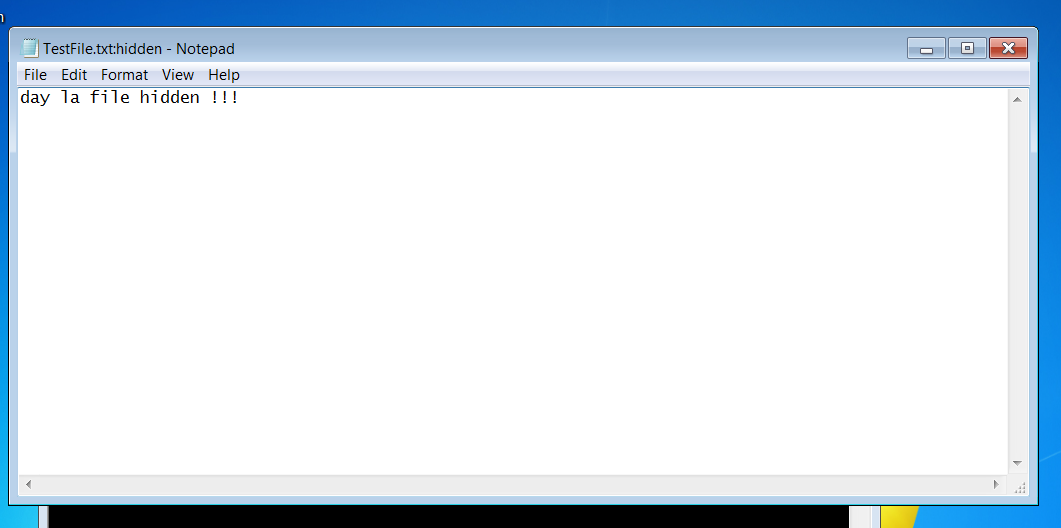
Kiểm tra kích thước tệp.



Ở dòng lệnh, nhập " **notepad Testfile.txt:hidden.txt**"

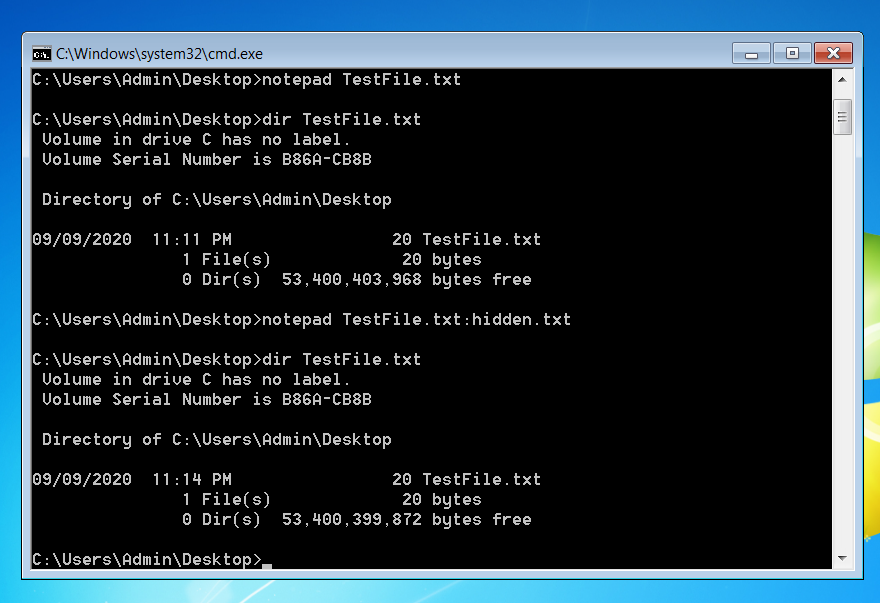


Nhập một số đoạn văn bản vào Notepad.

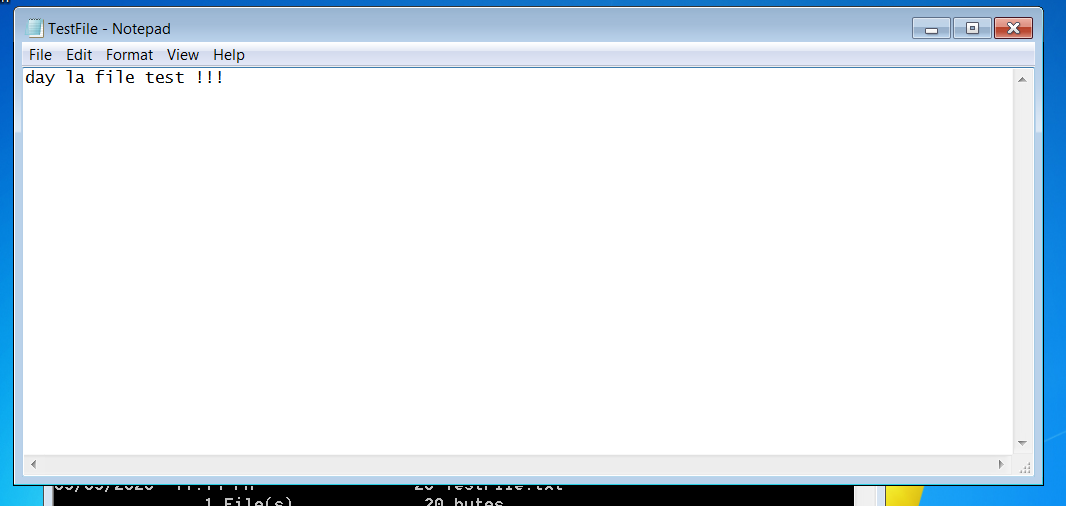


Lưu tệp và đóng lại.

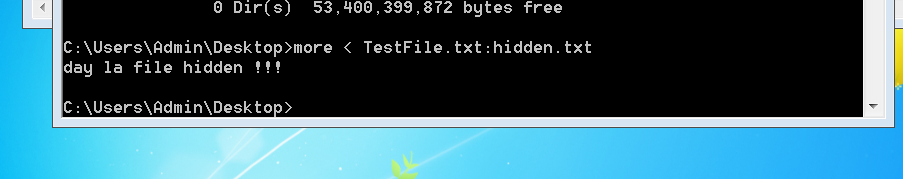
Kiểm tra kích thước tệp lần nữa (giống với kích thước ban đầu)



Mở**Test.txt**. Bạn sẽ chỉ thấy dữ liệu gốc.



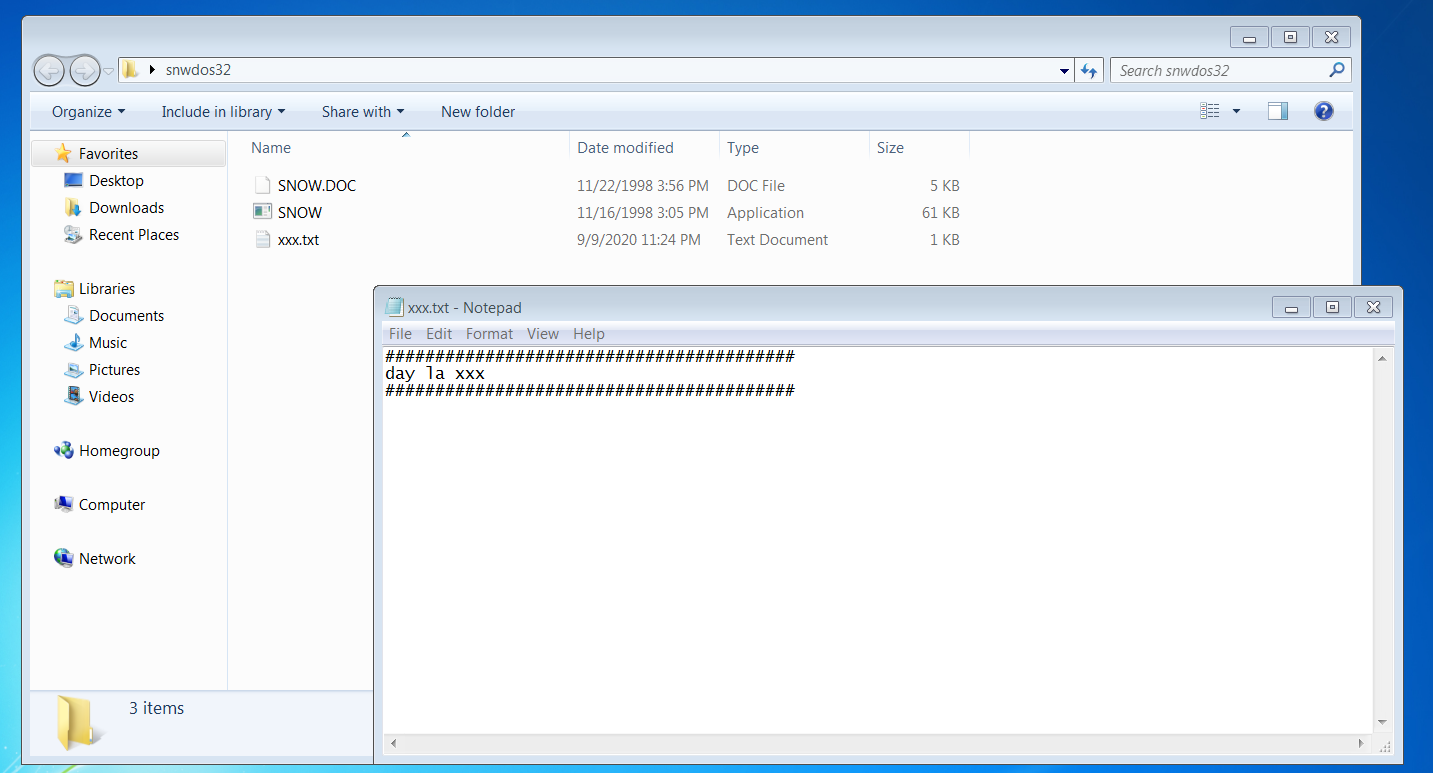
Nội dung file ẩn

Đối phó NTFS stream

Sử dụng công cụ và công nghệ từ bên thứ ba có thể chống lại **NTFS stream**. Phương pháp đơn giản nhất để ngăn chặn NTFS là chuyển tệp đáng nghi đến FAT. FAT không hỗ trợ dòng dữ liệu xen kẽ (ADS). Chuyển ADS từ NTFS đến FAT sẽ làm hỏng tệp. Có nhiều công cụ khác như ADS Spy, ADS Tools, LADS, Stream Armor có thể phát hiện và xóa tệp hoàn toàn.

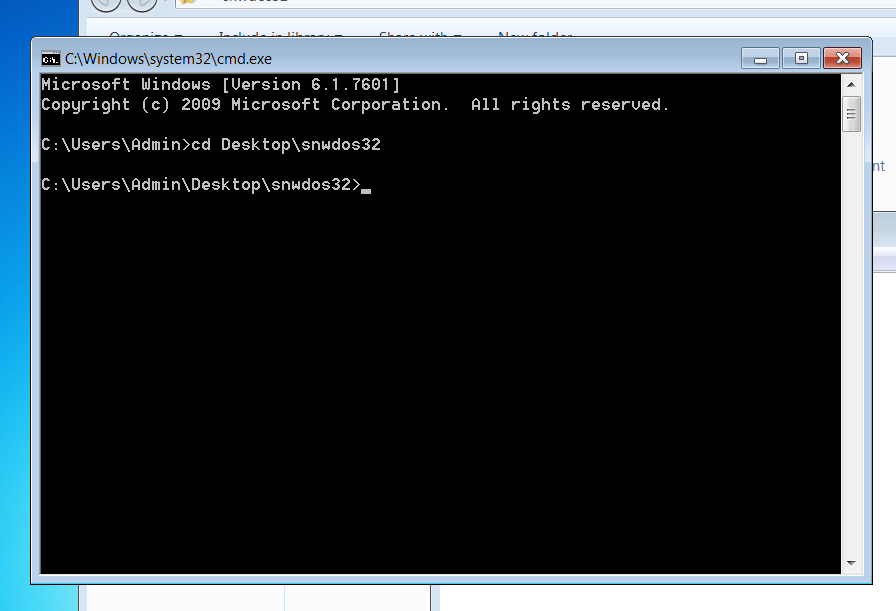
1. White Space Steganography

Tạo một tệp văn bản với dữ liệu trong cùng thư mục với **Snow Tool**.



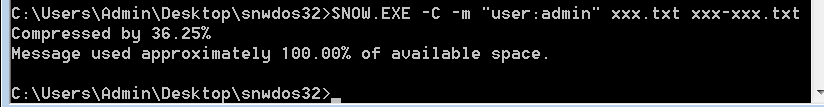
Đến **Command Prompt**.

Đổi thư mục để chạy **Snow Tool**.

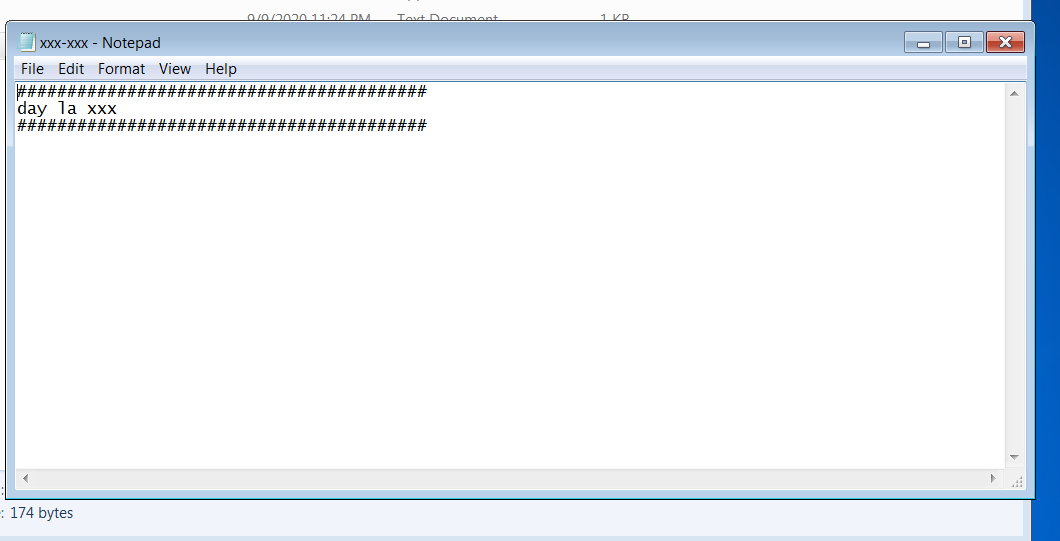


Nhập dòng lệnh **Snow –C –m “text to be hide” –p “password” <Sourcefile>  <Destinationfile>**

Tệp nguồn là tệp **xxx.txt**như trên. Tệp đến sẽ là copy của tệp nguồn chứa thông tin đã ẩn.

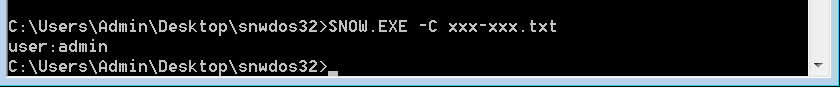


Đến thư mục, bạn sẽ thấy một tệp mới **xxx-xxx.txt**. Mở tệp.



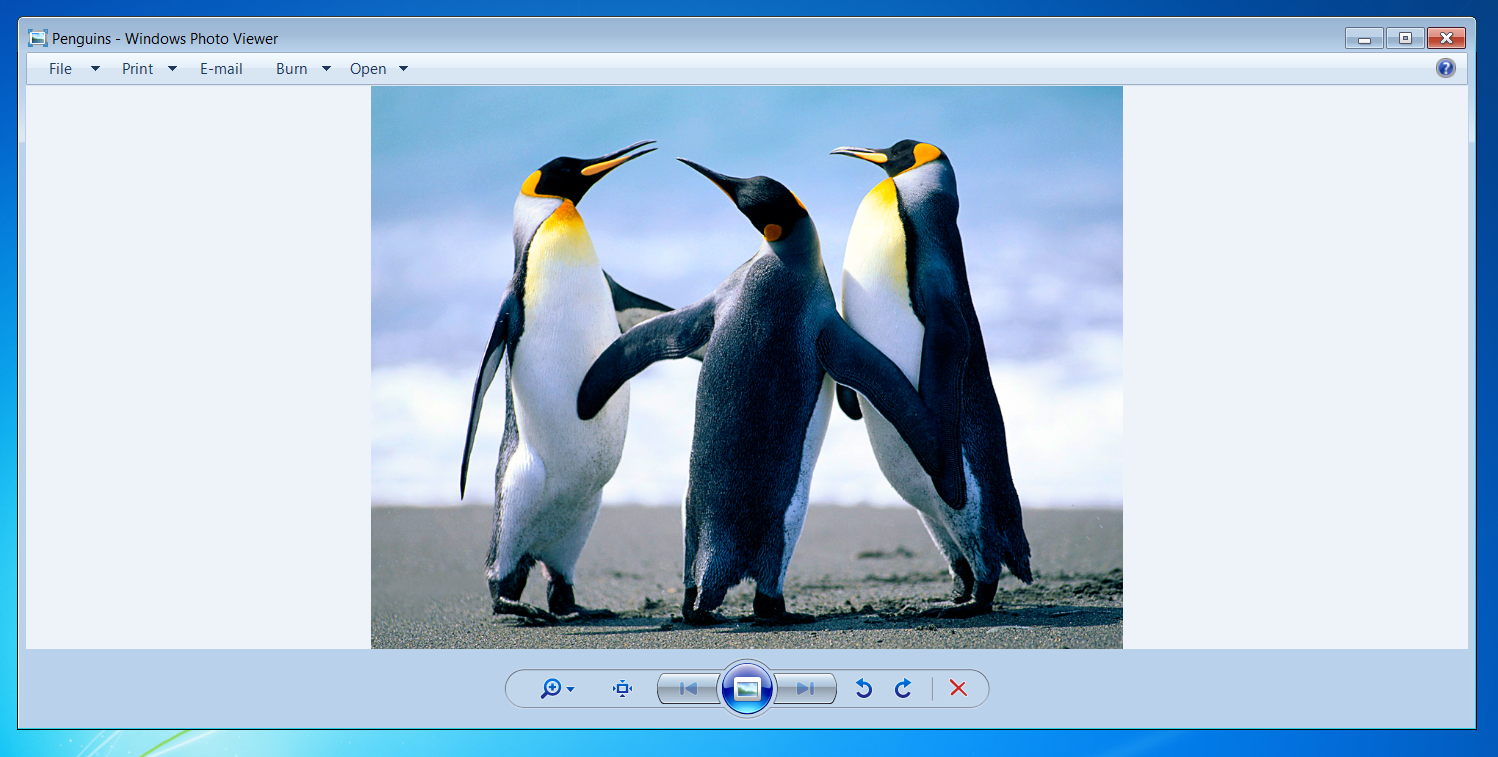
Tệp mới chứa văn bản như tệp gốc, không có thông tin ẩn nào.

Trích xuất dữ liệu ẩn.



1. Image Steganography

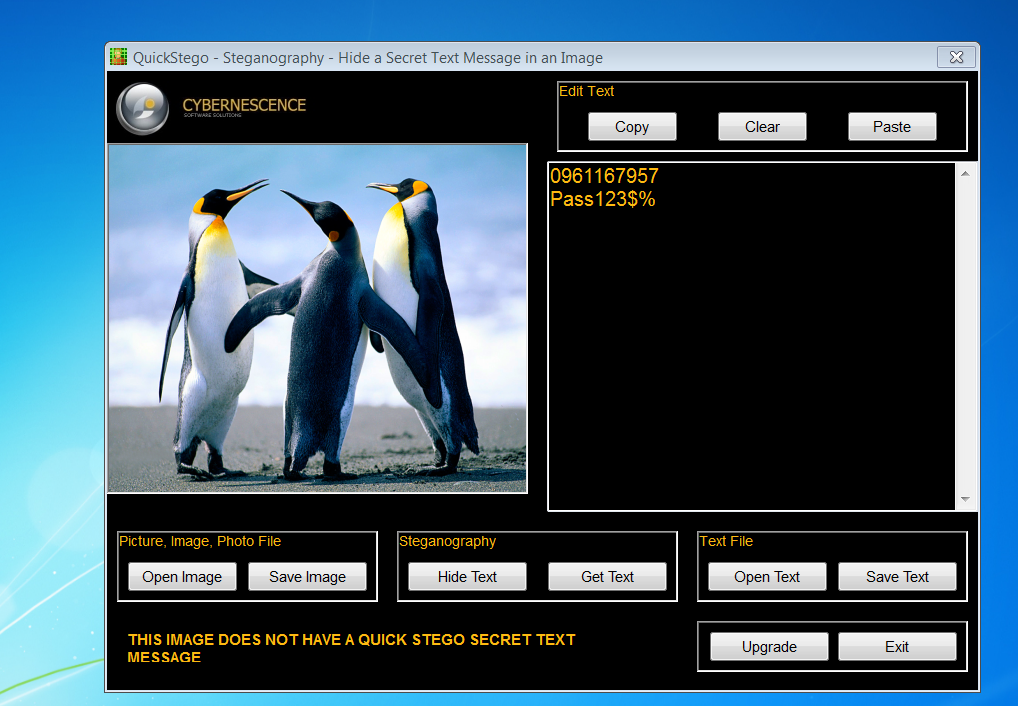
View ảnh chưa ẩn thông điệp



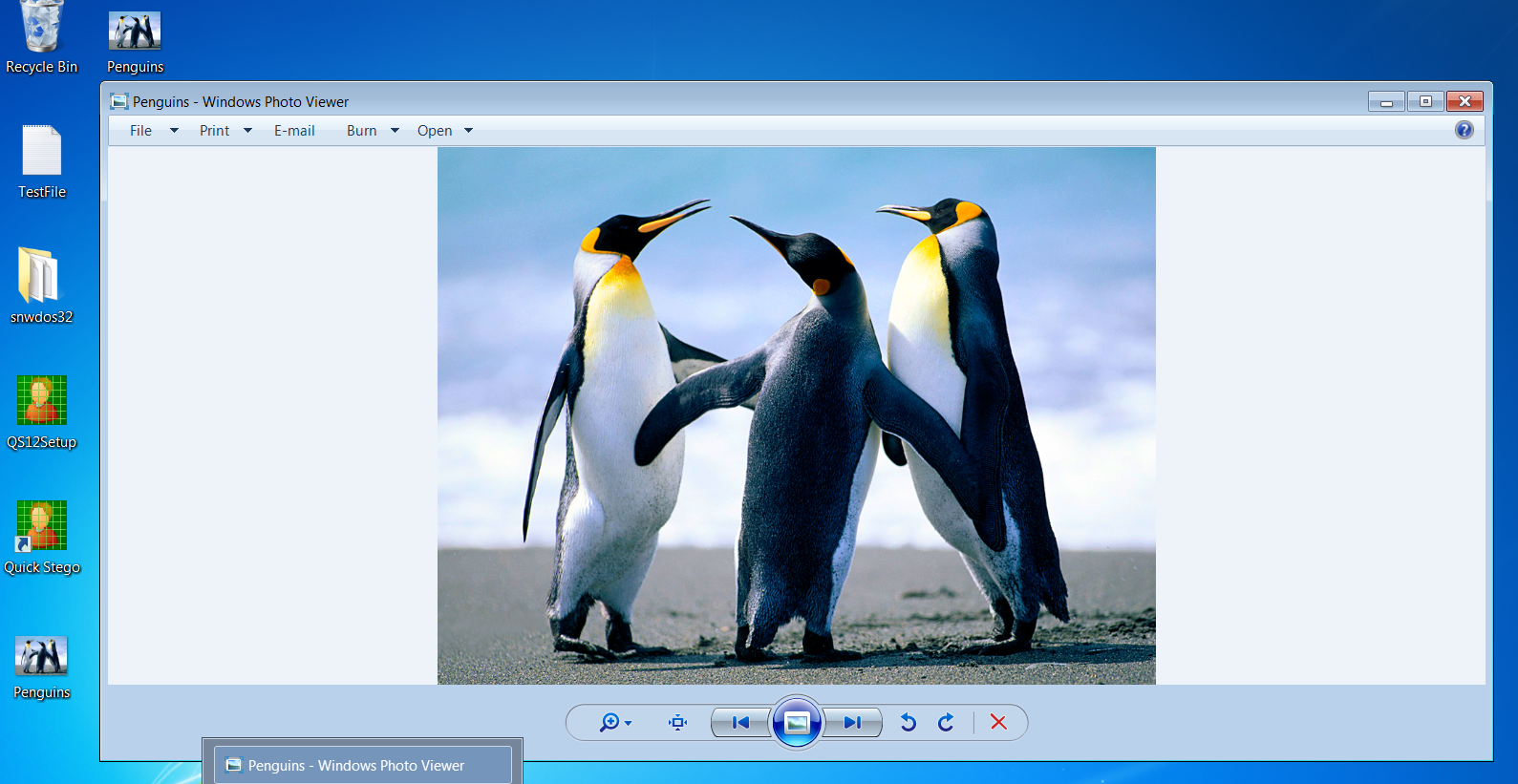
Khởi động tool Quick Stego chọn ảnh cần ẩn thông điệp



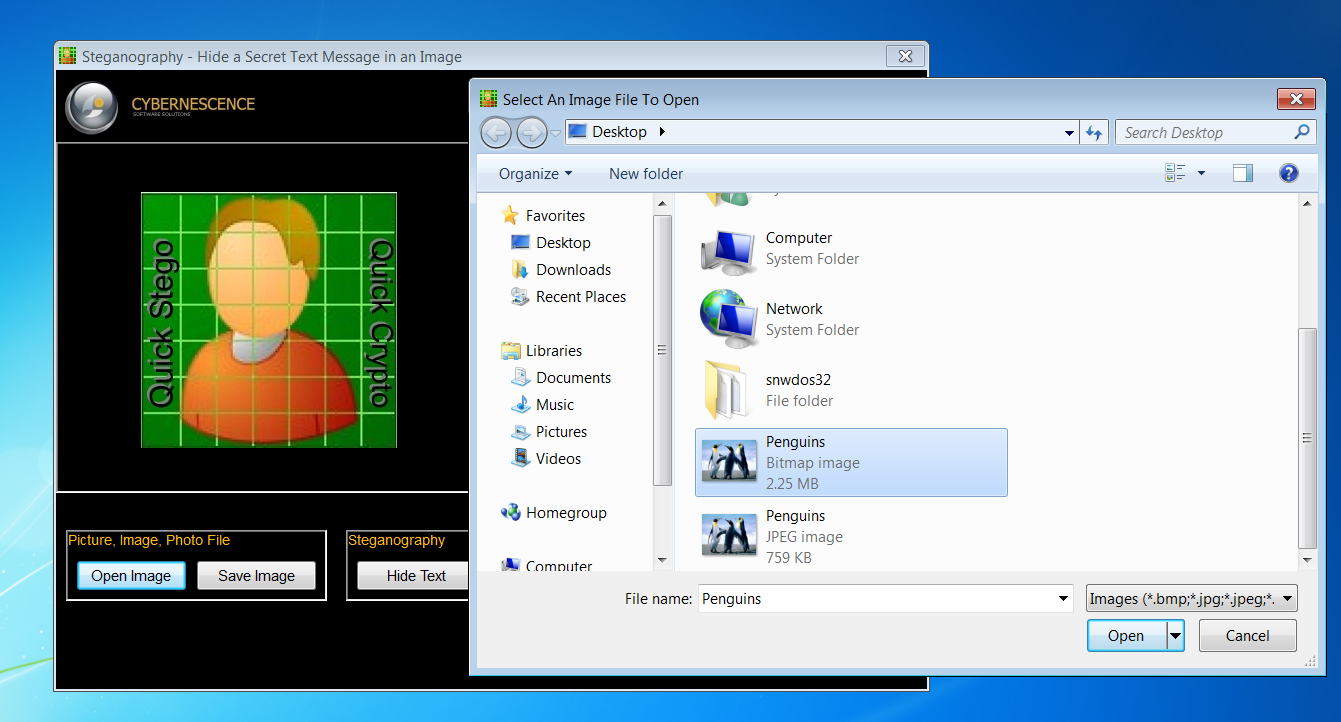
Chèn thông điệp vào ảnh chọn **Steganography Hide Text**

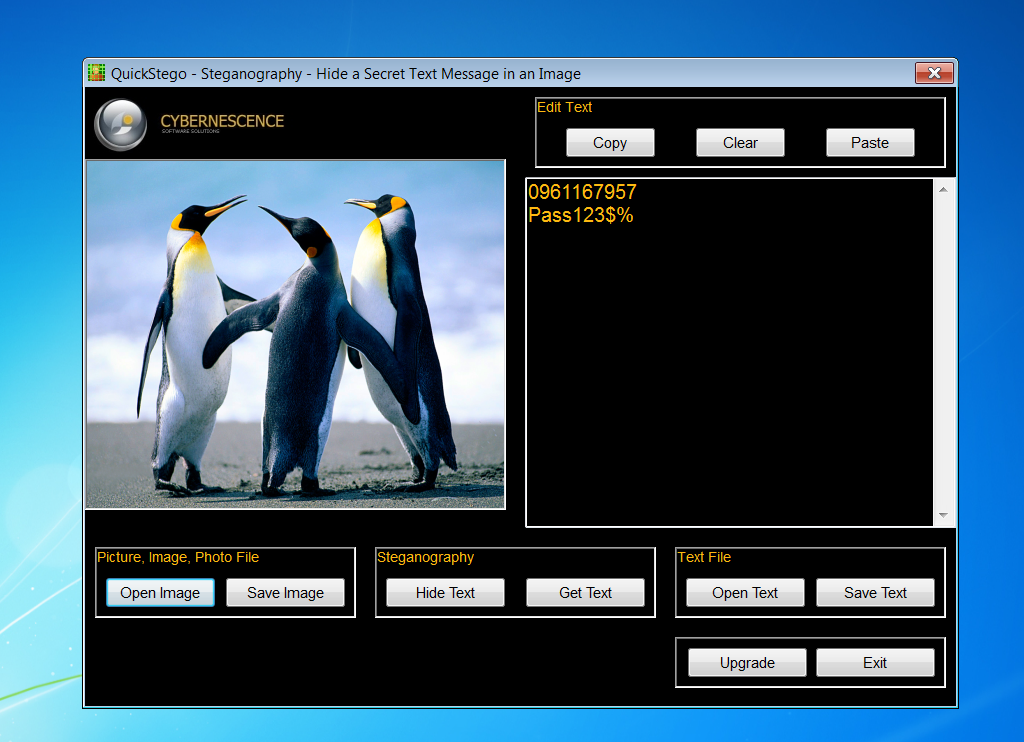


Save Image được ảnh Penguins.bmp



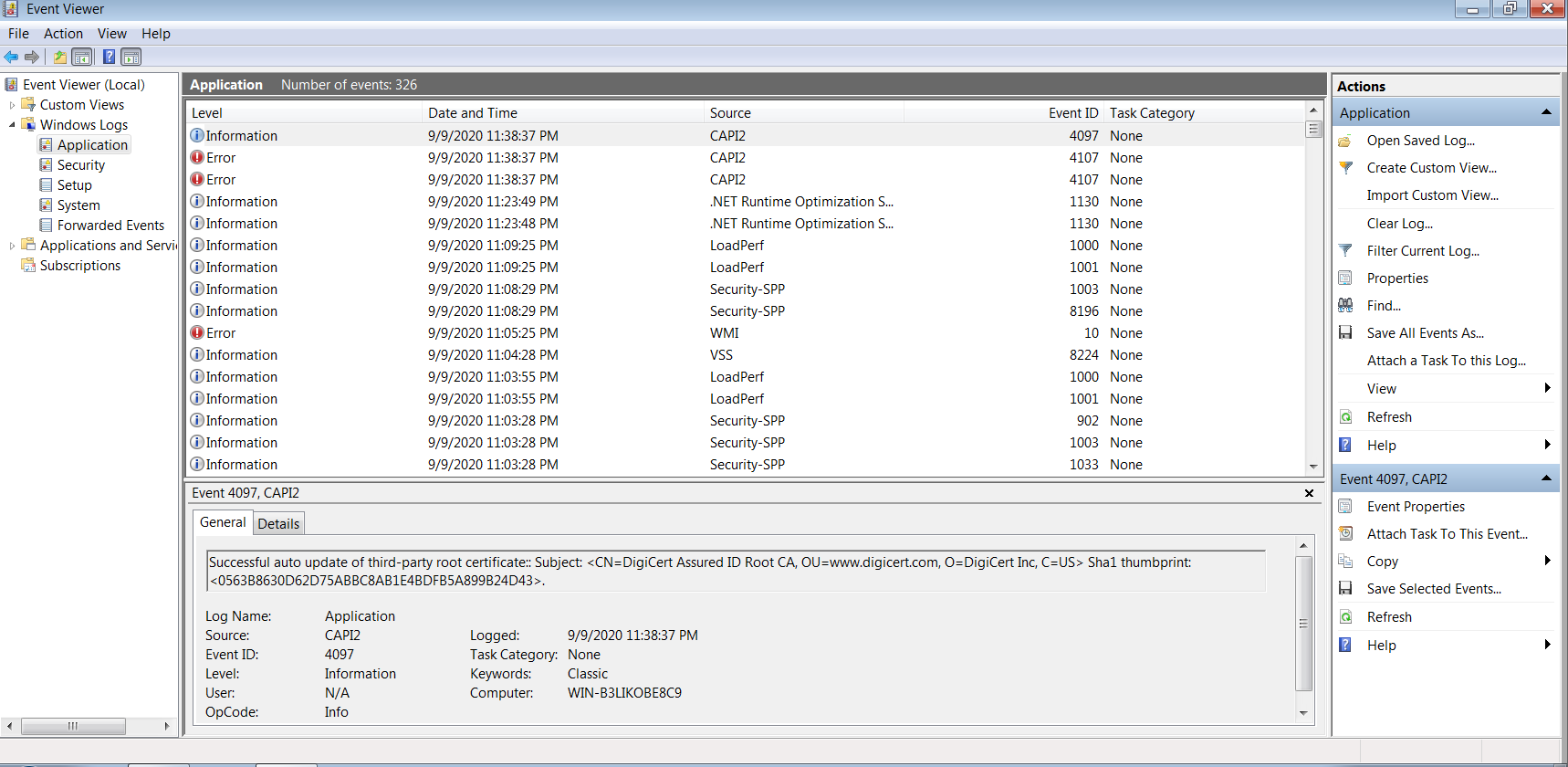
Khi mở ảnh mới tạo được bằng tool Quick Stego ta thu được thông tin ẩn trong ảnh





1. Clearing logs

Vào tool chọn thư mục Windows Logs



Chọn **Clear Log..** trong mục **Actions**

